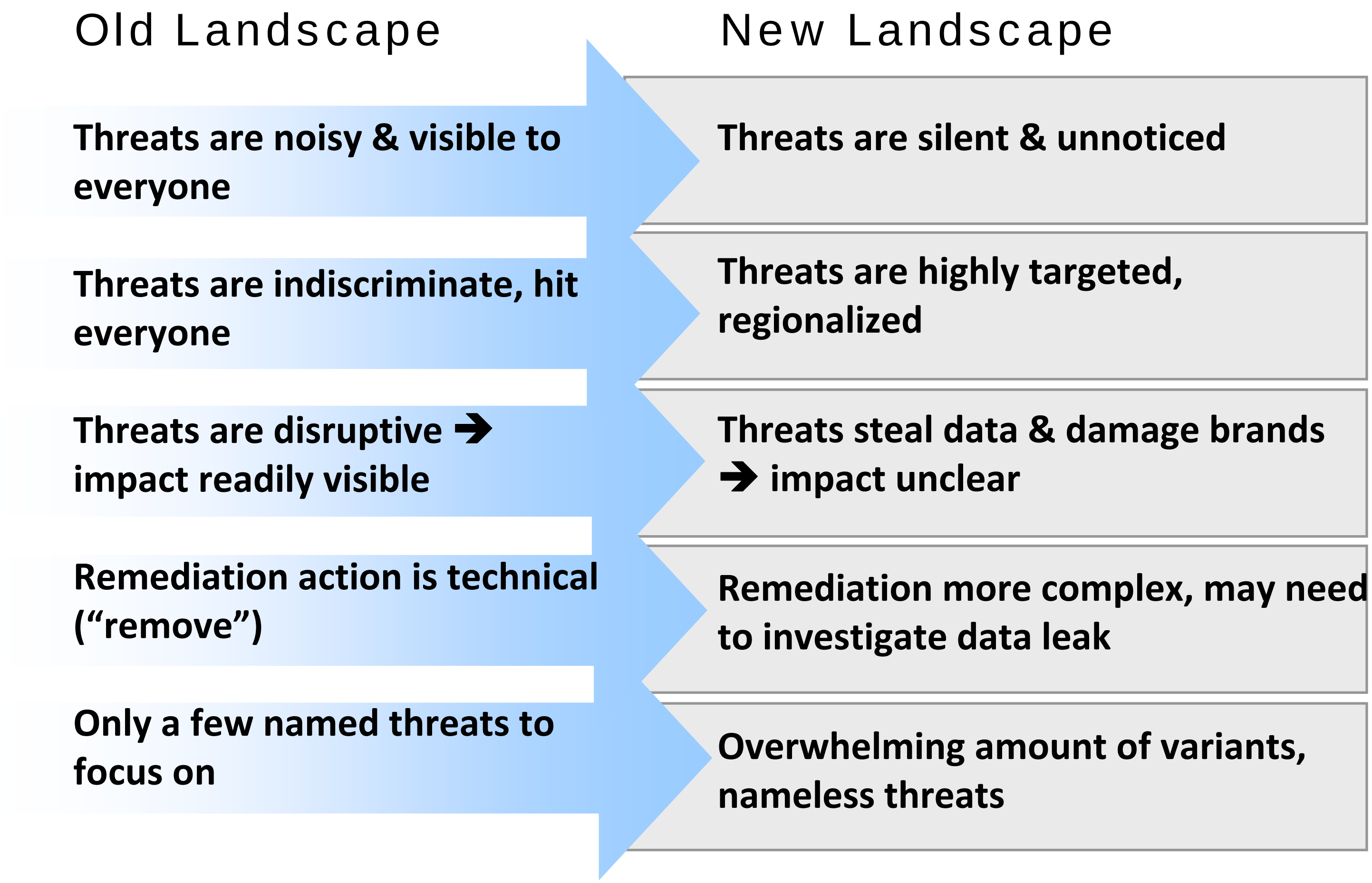
ELECTRONIC METHODS TO SPOT FRAUD AND EMBEZZLEMENT

Michael Allred
Information Security Manager
State of Utah
mwallred@utah.gov

Agenda

- Top threats today
  - Outsider threat
  - Insider threat
- What should you be looking for?
- Tools & Techniques

Threat Landscape Shift



Old Landscape	New Landscape
Threats are noisy & visible to everyone	Threats are silent & unnoticed
Threats are indiscriminate, hit everyone	Threats are highly targeted, regionalized
Threats are disruptive ➔ impact readily visible	Threats steal data & damage brands ➔ impact unclear
Remediation action is technical (“remove”)	Remediation more complex, may need to investigate data leak
Only a few named threats to focus on	Overwhelming amount of variants, nameless threats

Top Cyber Security Threats Today

- Exploit browser vulnerabilities – especially on trusted web sites
- Increased effectiveness in botnets
- Advanced identity theft from bots
- Attacks by well funded criminal organizations and countries
- Attacks against mobile devices such as iPhone and Android phones
- **Data loss from insider attacks and irresponsible users**
- Web application security exploits
- Increasingly malicious spyware
- **Sophisticated social engineering phishing**
- Infected consumer devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.) distributed by trusted organizations

Source SANS.ORG

Data Loss From Outside Attacks

- *Outside Threats*
  - *Target workstation more than servers*
  - *Bots and other malicious software*
  - *Criminal organizations with targeted attacks*
    - *Small time local criminals*
    - *Well funding criminal organizations*

Increasingly Malicious Spyware

- Spyware is a much bigger problem than many realize:
  - *90% of all Windows PCs are infected by spyware*
  - *80% of all home computers are infected by spyware*
  - *88% of owners of infected systems are not aware their computer is infected.*
  - *75% of PC owners believe they are safe from online threats.*
  - *Only 24% of PC owners are actually knowledgeable about how to handle spyware*
  - *65% of all PC users do not run up-to-date anti-virus software.*
  - *50% of all broadband users do not use a firewall. The number drops to 7% for dial-up users.*

According to Dell™ survey, Sep 17-19, 2004

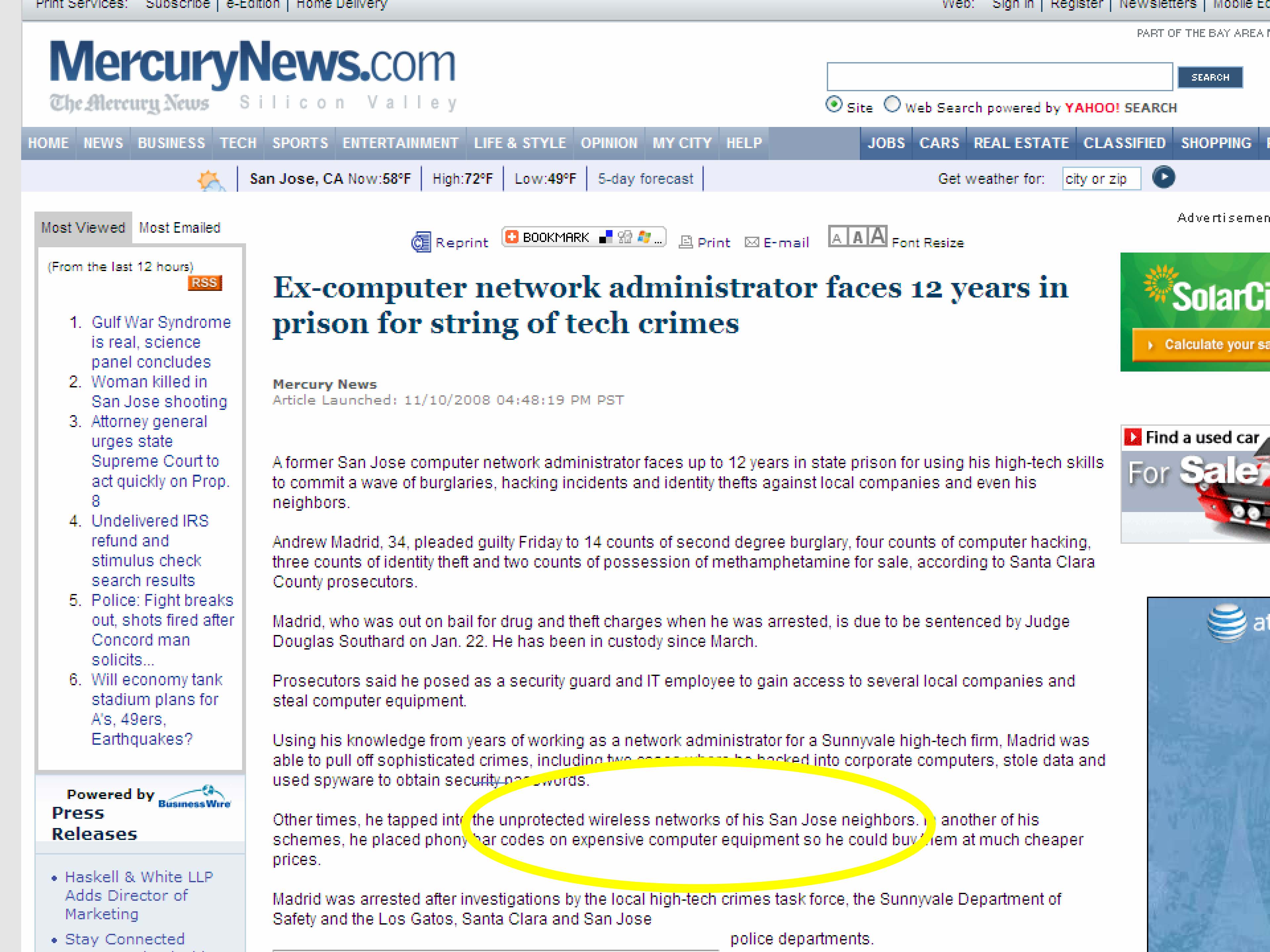
According to National Cyber Security Alliance and America Online™ survey, Oct 25, 2004

Increasingly Malicious Spyware

- Forms of Spyware
  - Browser Tracking
  - Information Theft
  - Key Logging
  - Dialers
  - Automatic Code Updaters
  - Spyware Security Holes

Data Loss From Insider Attacks

- *Insider threat*
  - *Deliberately Malicious*
    - *Theft of data by employees*
    - *Theft of equipment*
  - *Carelessly Malicious*
    - *Loss of USB drives and other media (backup tapes, CDs)*
    - *Used equipment being sold with data*
    - *Emailing data (credit cards, employee records)*
    - *Inappropriate web sites loading malicious code*



MercuryNews.com
The Mercury News Silicon Valley

SEARCH
● Site ○ Web Search powered by YAHOO! SEARCH

HOME | NEWS | BUSINESS | TECH | SPORTS | ENTERTAINMENT | LIFE & STYLE | OPINION | MY CITY | HELP | JOBS | CARS | REAL ESTATE | CLASSIFIED | SHOPPING

San Jose, CA Now:58°F | High:72°F | Low:49°F | 5-day forecast | Get weather for: city or zip

Most Viewed | Most Emailed

(From the last 12 hours) RSS

1. Gulf War Syndrome is real, science panel concludes
2. Woman killed in San Jose shooting
3. Attorney general urges state Supreme Court to act quickly on Prop. 8
4. Undelivered IRS refund and stimulus check search results
5. Police: Fight breaks out, shots fired after Concord man solicits...
6. Will economy tank stadium plans for A's, 49ers, Earthquakes?

Powered by BusinessWire
Press Releases

- Haskell & White LLP Adds Director of Marketing
- Stay Connected

Reprint | BOOKMARK | Print | E-mail | A A A Font Resize

Ex-computer network administrator faces 12 years in prison for string of tech crimes

Mercury News
Article Launched: 11/10/2008 04:48:19 PM PST

A former San Jose computer network administrator faces up to 12 years in state prison for using his high-tech skills to commit a wave of burglaries, hacking incidents and identity thefts against local companies and even his neighbors.

Andrew Madrid, 34, pleaded guilty Friday to 14 counts of second degree burglary, four counts of computer hacking, three counts of identity theft and two counts of possession of methamphetamine for sale, according to Santa Clara County prosecutors.

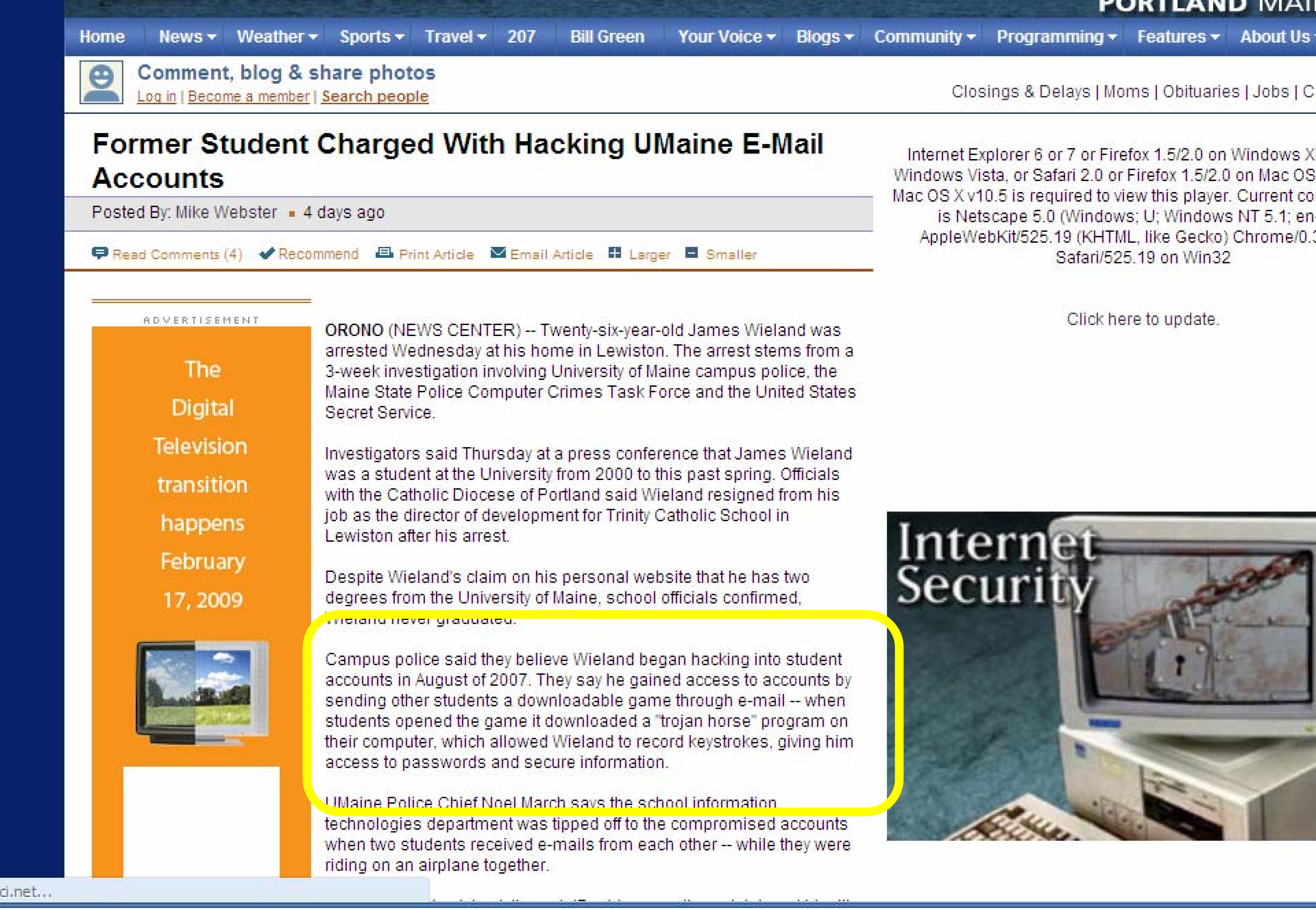
Madrid, who was out on bail for drug and theft charges when he was arrested, is due to be sentenced by Judge Douglas Southard on Jan. 22. He has been in custody since March.

Prosecutors said he posed as a security guard and IT employee to gain access to several local companies and steal computer equipment.

Using his knowledge from years of working as a network administrator for a Sunnyvale high-tech firm, Madrid was able to pull off sophisticated crimes, including two cases where he hacked into corporate computers, stole data and used spyware to obtain security passwords.

Other times, he tapped into the unprotected wireless networks of his San Jose neighbors. In another of his schemes, he placed phony bar codes on expensive computer equipment so he could buy them at much cheaper prices.

Madrid was arrested after investigations by the local high-tech crimes task force, the Sunnyvale Department of Safety and the Los Gatos, Santa Clara and San Jose police departments.



Comment, blog & share photos
Log in | Become a member | Search people

Closings & Delays | Moms | Obituaries | Jobs | C

Former Student Charged With Hacking UMaine E-Mail Accounts

Posted By: Mike Webster ▪ 4 days ago

Read Comments (4) ✓ Recommend Print Article Email Article Larger Smaller

ORONO (NEWS CENTER) -- Twenty-six-year-old James Wieland was arrested Wednesday at his home in Lewiston. The arrest stems from a 3-week investigation involving University of Maine campus police, the Maine State Police Computer Crimes Task Force and the United States Secret Service.

Investigators said Thursday at a press conference that James Wieland was a student at the University from 2000 to this past spring. Officials with the Catholic Diocese of Portland said Wieland resigned from his job as the director of development for Trinity Catholic School in Lewiston after his arrest.

Despite Wieland's claim on his personal website that he has two degrees from the University of Maine, school officials confirmed, Wieland never graduated.

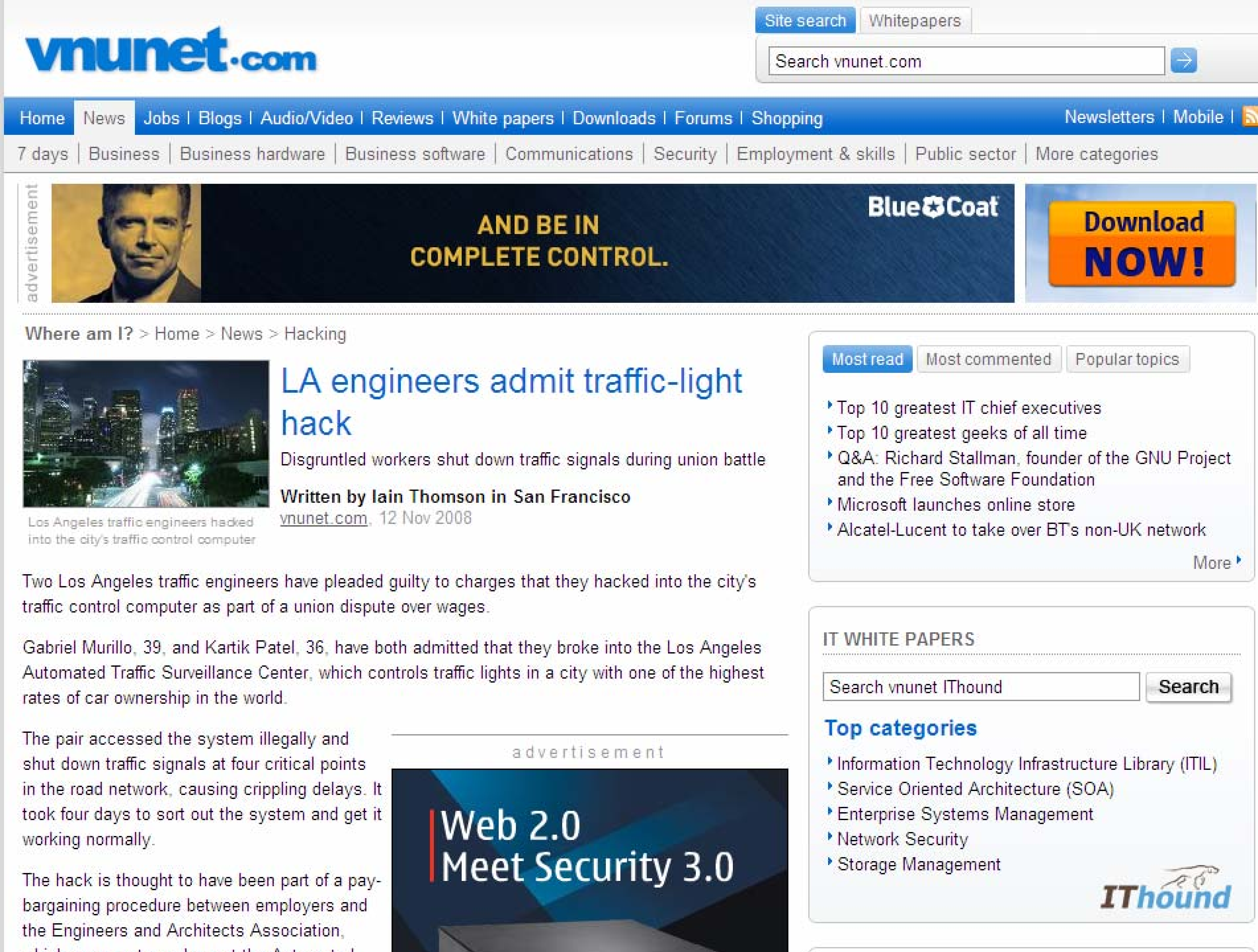
Campus police said they believe Wieland began hacking into student accounts in August of 2007. They say he gained access to accounts by sending other students a downloadable game through e-mail -- when students opened the game it downloaded a "trojan horse" program on their computer, which allowed Wieland to record keystrokes, giving him access to passwords and secure information.

UMaine Police Chief Noel March says the school information technologies department was tipped off to the compromised accounts when two students received e-mails from each other -- while they were riding on an airplane together.

Internet Explorer 6 or 7 or Firefox 1.5/2.0 on Windows X Windows Vista, or Safari 2.0 or Firefox 1.5/2.0 on Mac OS Mac OS X v10.5 is required to view this player. Current co is Netscape 5.0 (Windows; U; Windows NT 5.1; en- AppleWebKit/525.19 (KHTML, like Gecko) Chrome/0.3 Safari/525.19 on Win32

Click here to update.

ci.net...



LA engineers admit traffic-light hack

Disgruntled workers shut down traffic signals during union battle

Written by Iain Thomson in San Francisco

vnunet.com, 12 Nov 2008

Los Angeles traffic engineers hacked into the city's traffic control computer

Two Los Angeles traffic engineers have pleaded guilty to charges that they hacked into the city's traffic control computer as part of a union dispute over wages.

Gabriel Murillo, 39, and Kartik Patel, 36, have both admitted that they broke into the Los Angeles Automated Traffic Surveillance Center, which controls traffic lights in a city with one of the highest rates of car ownership in the world.

The pair accessed the system illegally and shut down traffic signals at four critical points in the road network, causing crippling delays. It took four days to sort out the system and get it working normally.

The hack is thought to have been part of a pay-bargaining procedure between employers and the Engineers and Architects Association,

Most read | Most commented | Popular topics

- Top 10 greatest IT chief executives
- Top 10 greatest geeks of all time
- Q&A: Richard Stallman, founder of the GNU Project and the Free Software Foundation
- Microsoft launches online store
- Alcatel-Lucent to take over BT's non-UK network

More

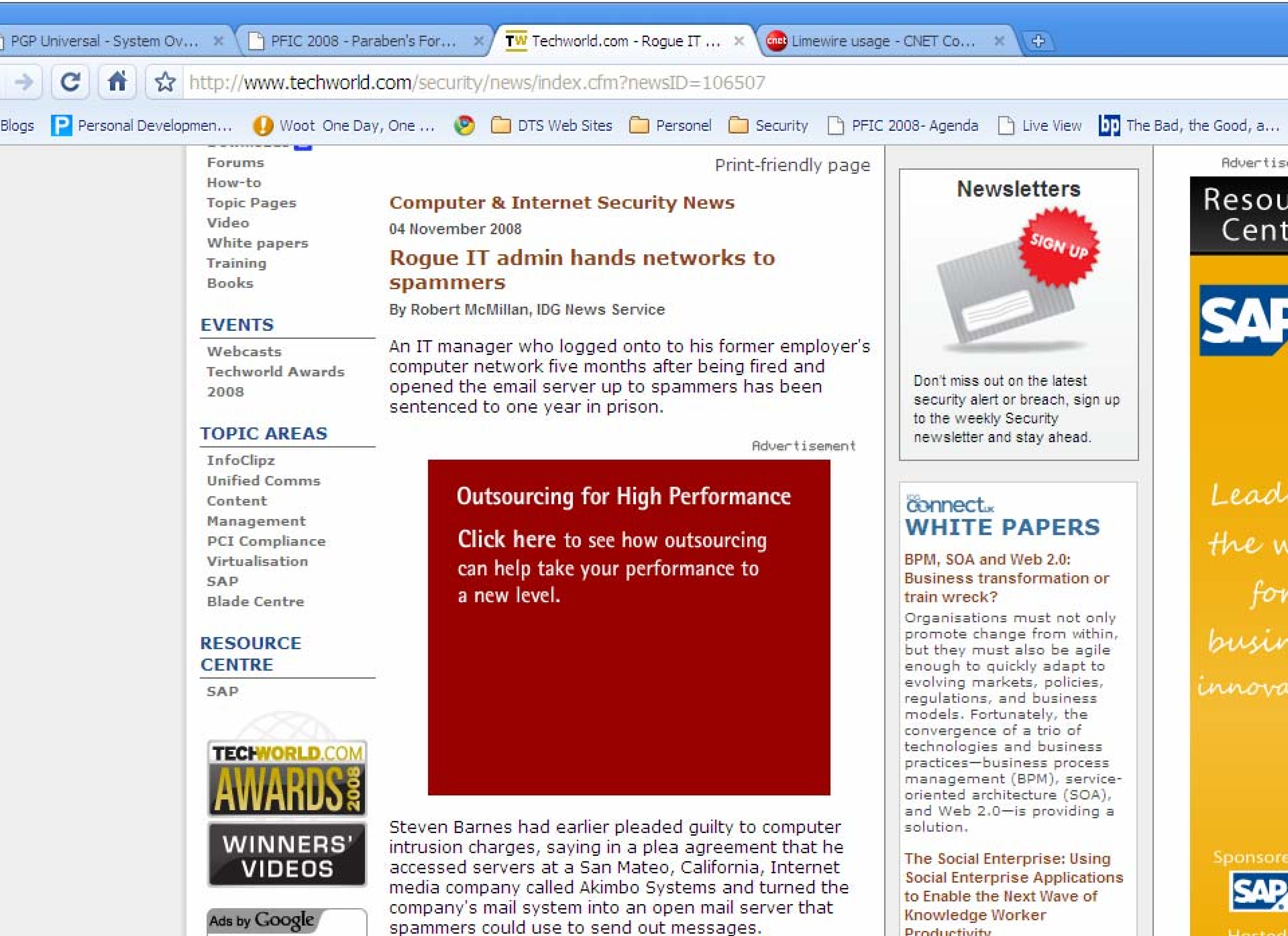
IT WHITE PAPERS

Search vnunet IThound | Search

Top categories

- Information Technology Infrastructure Library (ITIL)
- Service Oriented Architecture (SOA)
- Enterprise Systems Management
- Network Security
- Storage Management

IThound



Computer & Internet Security News

04 November 2008

Rogue IT admin hands networks to spammers

By Robert McMillan, IDG News Service

An IT manager who logged onto to his former employer's computer network five months after being fired and opened the email server up to spammers has been sentenced to one year in prison.

Steven Barnes had earlier pleaded guilty to computer intrusion charges, saying in a plea agreement that he accessed servers at a San Mateo, California, Internet media company called Akimbo Systems and turned the company's mail system into an open mail server that spammers could use to send out messages.

Newsletters

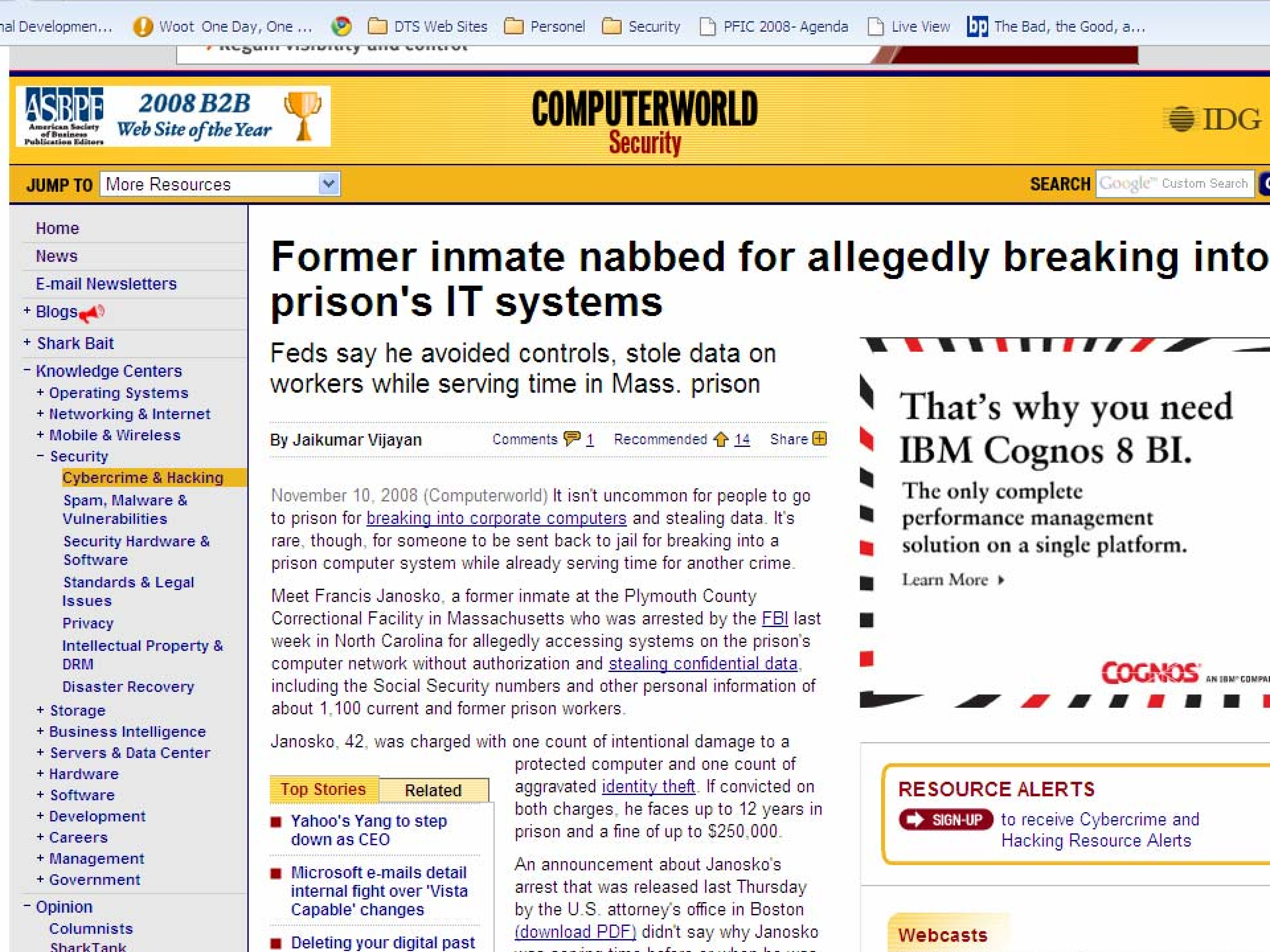
Don't miss out on the latest security alert or breach, sign up to the weekly Security newsletter and stay ahead.

IDG connect.uk WHITE PAPERS

BPM, SOA and Web 2.0: Business transformation or train wreck?

Organisations must not only promote change from within, but they must also be agile enough to quickly adapt to evolving markets, policies, regulations, and business models. Fortunately, the convergence of a trio of technologies and business practices—business process management (BPM), service-oriented architecture (SOA), and Web 2.0—is providing a solution.

The Social Enterprise: Using Social Enterprise Applications to Enable the Next Wave of Knowledge Worker Productivity



nal Developmen... Woot One Day, One ... DTS Web Sites Personel Security PFIC 2008- Agenda Live View The Bad, the Good, a...

COMPUTERWORLD
Security
IDG

JUMP TO More Resources
SEARCH Google™ Custom Search

Home
News
E-mail Newsletters
+ Blogs
+ Shark Bait
- Knowledge Centers
+ Operating Systems
+ Networking & Internet
+ Mobile & Wireless
- Security
Cybercrime & Hacking
Spam, Malware & Vulnerabilities
Security Hardware & Software
Standards & Legal Issues
Privacy
Intellectual Property & DRM
Disaster Recovery
+ Storage
+ Business Intelligence
+ Servers & Data Center
+ Hardware
+ Software
+ Development
+ Careers
+ Management
+ Government
- Opinion
Columnists
SharkTank

Former inmate nabbed for allegedly breaking into prison's IT systems

Feds say he avoided controls, stole data on workers while serving time in Mass. prison

By Jaikumar Vijayan

November 10, 2008 (Computerworld) It isn't uncommon for people to go to prison for breaking into corporate computers and stealing data. It's rare, though, for someone to be sent back to jail for breaking into a prison computer system while already serving time for another crime.

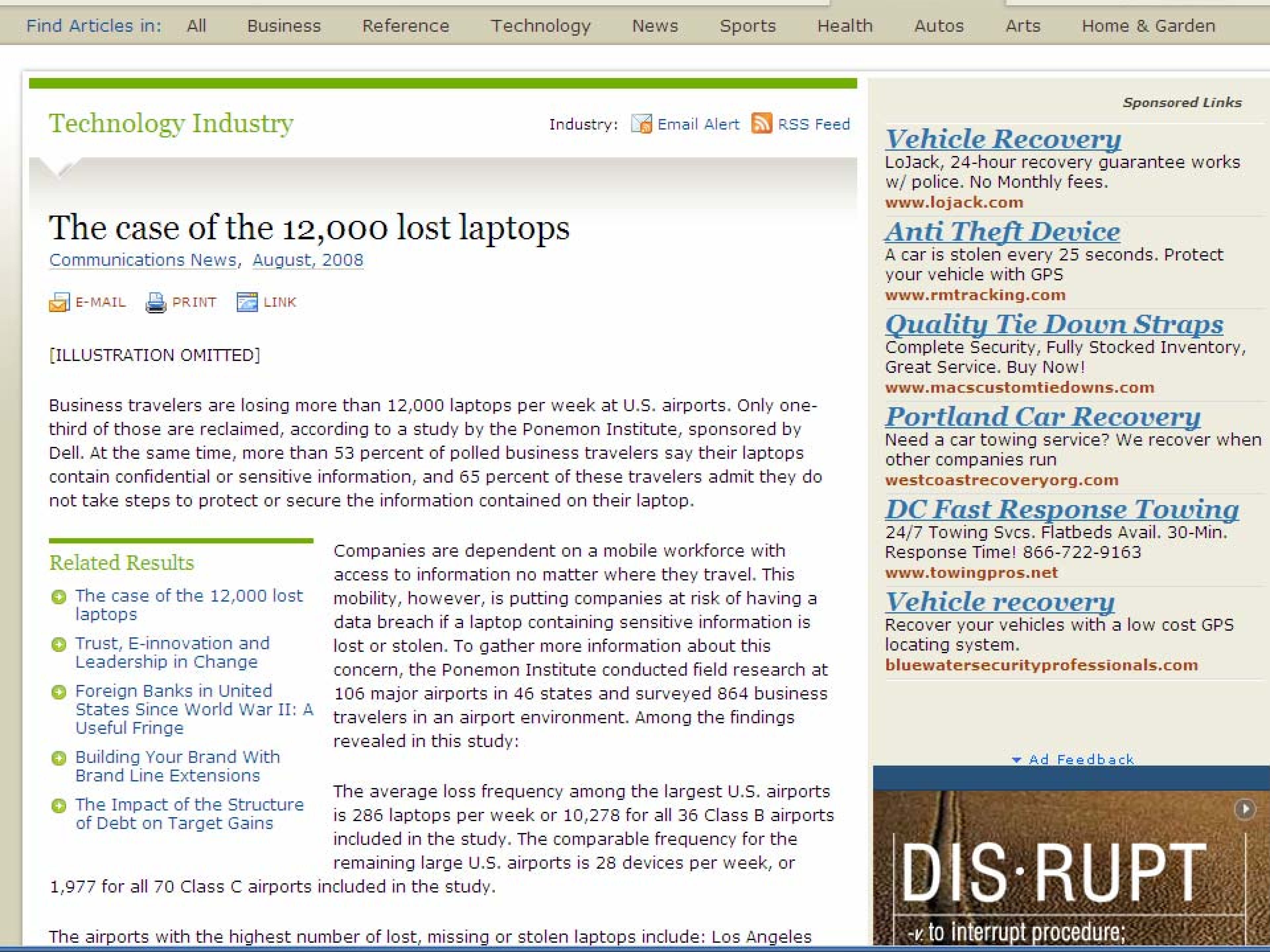
Meet Francis Janosko, a former inmate at the Plymouth County Correctional Facility in Massachusetts who was arrested by the FBI last week in North Carolina for allegedly accessing systems on the prison's computer network without authorization and stealing confidential data, including the Social Security numbers and other personal information of about 1,100 current and former prison workers.

Janosko, 42, was charged with one count of intentional damage to a protected computer and one count of aggravated identity theft. If convicted on both charges, he faces up to 12 years in prison and a fine of up to $250,000.

An announcement about Janosko's arrest that was released last Thursday by the U.S. attorney's office in Boston (download PDF) didn't say why Janosko

Top Stories Related
Yahoo's Yang to step down as CEO
Microsoft e-mails detail internal fight over 'Vista Capable' changes
Deleting your digital past

Webcasts



Technology Industry

Industry: Email Alert RSS Feed

The case of the 12,000 lost laptops

Communications News, August, 2008

E-MAIL PRINT LINK

[ILLUSTRATION OMITTED]

Business travelers are losing more than 12,000 laptops per week at U.S. airports. Only one-third of those are reclaimed, according to a study by the Ponemon Institute, sponsored by Dell. At the same time, more than 53 percent of polled business travelers say their laptops contain confidential or sensitive information, and 65 percent of these travelers admit they do not take steps to protect or secure the information contained on their laptop.

Related Results

- The case of the 12,000 lost laptops
- Trust, E-innovation and Leadership in Change
- Foreign Banks in United States Since World War II: A Useful Fringe
- Building Your Brand With Brand Line Extensions
- The Impact of the Structure of Debt on Target Gains

Companies are dependent on a mobile workforce with access to information no matter where they travel. This mobility, however, is putting companies at risk of having a data breach if a laptop containing sensitive information is lost or stolen. To gather more information about this concern, the Ponemon Institute conducted field research at 106 major airports in 46 states and surveyed 864 business travelers in an airport environment. Among the findings revealed in this study:

The average loss frequency among the largest U.S. airports is 286 laptops per week or 10,278 for all 36 Class B airports included in the study. The comparable frequency for the remaining large U.S. airports is 28 devices per week, or 1,977 for all 70 Class C airports included in the study.

The airports with the highest number of lost, missing or stolen laptops include: Los Angeles

Data Loss From Insider Attacks

- *State, Federal and Industry Regulations*
  - *HIPAA Healthcare*
  - *PCI Payment Card Industry*
  - *SOX Financial*
  - *GBLA Banking*

Insider Threats Triggers

- *Negative work-related event triggers most insiders' actions*
- *Most had acted out previously*
- *Majority had system administrator privilege rights*
- *Used unsophisticated methods to exploit systems*
- *Used compromised accounts, created backdoors or shared accounts*
- *Remote access was used to carry out attacks*
- *Only detected because system became unavailable*
- *Caused financial losses, impacted operations or damaged reputations*

Source: U.S. Secret Service and CERT
Coordination Center
May 2005

Data Loss From Insider Attacks

- *Detection*
  - *Employees need to report all suspicious activity*
  - *Logging and monitoring*
  - *Watching for “weirdness factor”*
    - *Outbound FTP/P2P*
    - *Email*
  - *Event correlation and system log aggregation*
    - *Users logging in from different IP addresses*
    - *Different login ids from same IP address*

Data Loss From Insider Attacks

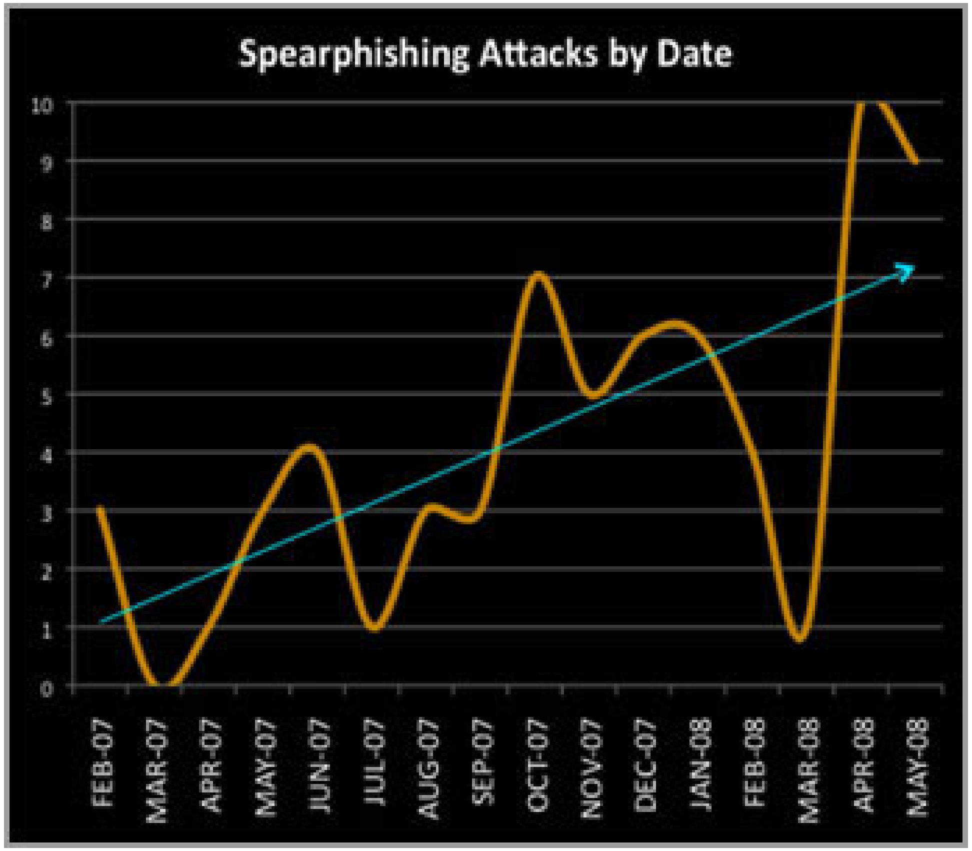
- *Wireless Access Threats*
  - *User adds their own wireless access point to your network*
    - *Can you detect it?*
  - *Don’t use WEP*
  - *Don’t let Windows connect to any wireless access point*
    - *Hotels, café, airports etc..*

Data Loss From Insider Attacks

- *What can be done?*
  - *User awareness and education*
  - *Acceptable use policies*
  - *Wiping old equipment before being resold*
  - *End Point software that prevents copying of data*
  - *Logging of systems and data accessed by users*
  - *Proper Authentication, Authorization and Accountability*
  - *Encryption of devices (mobile, USB, laptops)*

Social Engineering Attacks

- Sophisticated Blending Phishing with VOIP
- Spearphishing
  - Highly targeted phishing attacks
- Whaling Attacks
  - Targeted at high value end users



Source iDefense June 7, 2008

Tips to avoid phishing scams

- Never reveal personal or financial information in a response to an email request, no matter who appears to have sent it.
- If you receive an e-mail message that appears suspicious, call the person or organization listed in the From line before you respond or open any attached files.
- Never click links in an email message that requests personal or financial information. Enter the Web address into your browser window instead.
- Don't post any information on your blog or social networking site that could be used by identity thieves to target you, your family or friends, or your company.
- Report any email that you suspect might be spear phishing within your company.
- Use a browser like Internet Explorer 7 or Firefox with Phishing Filters.

Conclusion

- Be careful out there
- Log and monitor as much as possible
- Review those logs
- Educate yourself about the risk
- Keep your system updated
- Someone really does want to steal your password
- Don’t disclose too much personal information online
- Used strong passwords
  - Palin’s email account high jacked